Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	WC Docket No. 18-89

COMMENTS OF THE
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)[1]

CCIA respectfully submits these Comments in the above-referenced proceeding.[2] CCIA appreciates the Commission's interest in protecting communications networks in the United States and addressing potential vulnerabilities in the supply chain for components and technologies that enable the country's robust networks. Before pursuing the action proposed in this NPRM, the Commission should understand the extent to which there are problems or vulnerabilities on networks in the U.S., and the extent to which they derive from components and technologies produced by companies like China's Huawei and ZTE. The Commission should narrow the scope of its rules to address vulnerabilities that may exist, and it should provide greater clarity to minimize disruption. Ultimately, given the number of open questions presented in this NPRM, the Commission should better define its policy options by issuing a Further Notice of Proposed Rulemaking.

[1] CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion. A list of CCIA's members is available online at http://www.ccianet.org/members.

[2] *Protecting against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, (Apr. 17, 2018) [hereinafter NPRM].

I. The Commission Should Assess the Prevalence of and Risks Associated with Huawei and ZTE Technology in the United States.

Much of the NPRM centers around the premise that there are vulnerabilities in Huawei and ZTE equipment and services that could allow the Chinese government and hostile entities to siphon off user data and gain critical information about the United States.[3] The Commission relies on a 2012 report from the House Permanent Select Committee on Intelligence (HPSCI) to support this notion.[4] While the report does not offer specific information on security threats that can be assessed and mitigated, it does explain political problems that have led to distrust of Huawei and ZTE.[5] The report notes that both Huawei and ZTE did not provide all of the information that HPSCI requested, and the information provided was not sufficient to satisfy the Committee.[6]

More recently, senior officials in the FBI, CIA, and NSA have urged the American public not to use Huawei products.[7] The Pentagon has banned the sale of both Huawei and ZTE handsets on military bases, noting the devices "may pose an unacceptable risk to the department's personnel, information and mission."[8] In response to ZTE's violation of the sanctions placed on North Korea and Iran, the U.S. Department of Commerce promulgated an

[3] *Id*. at ¶¶ 4-6.
[4] *Id*. at ¶ 4.
[5] House of Representatives Select Permanent Committee on Intelligence, 112th Cong., Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE 11-12, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.
[6] *Id*. at 12-13, 21-25.
[7] Chaim Gartenberg, *Best Buy Won't Sell Huawei Phones, Laptops, or Smartwatches Anymore*, THE VERGE (Mar. 22, 2018), https://www.theverge.com/2018/3/22/17151186/best-buy-huawei-smartphone-china; James Vincent, *Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA*, THE VERGE (Feb. 14, 2018), https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears.
[8] Katie Collins, *Pentagon Bans Sale of Huawei, ZTE Phones on US Military Bases*, CNET (May 2, 2018), https://www.cnet.com/news/pentagon-reportedly-bans-sale-of-huawei-and-zte-phones-on-us-military-bases/.

export ban preventing U.S. firms from doing business with ZTE for seven years.[9] Last year, ZTE was fined over $1 billion by the United States, which was the largest ever penalty levied in an export control case.[10] After the export ban was levied against ZTE, few to none of its products made their way into the United States.[11]

Parts of the United States government are concerned about ingress by Huawei and ZTE into the U.S. market for communications equipment as well as allowing the Chinese governmnet a backdoor into the country's critical infrastructure. However, the U.S. market shares of Huawei and ZTE are relatively small compared to the rest of the world.[12] Huawei may be better known internationally not for selling handsets, but for selling network infrastructure equipment, like network switches and relays.[13] Indeed, longtime leaders in telecommunications equipment, Ericsson and Nokia, are struggling to compete with newer Chinese competitors, like Huawei, which "is now the world's biggest seller of the networking gear at the center of modern mobile communications—even though it hasn't made much headway in U.S."[14] Most network equipment manufactured by Huawei that is brought into the U.S. is not used by the larger communications service providers. Rather, it is used by regional or local providers (likely those that receive Universal Service Fund (USF) support) that may not have the funds to buy more

[9] David Lynch, *U.S. Companies Banned From Selling To China's ZTE Telecom Maker*, THE WASH. POST (Apr. 16, 2018), https://www.washingtonpost.com/news/business/wp/2018/04/16/u-s-companies-banned-from-selling-to-chinas-zte-telecom-maker/.

[10] *Id*.

[11] Ron Amadeo, *ZTE Exports Ban May Mean No Google Apps, a Death Sentence for Its Smartphones*, ARS TECHNICA (Apr. 18, 2018), https://arstechnica.com/gadgets/2018/04/googles-us-android-go-launch-derailed-by-zte-ban/.

[12] Apple Passes Samsung to Capture the Top Position in the Worldwide Smartphone Market While Overall Shipments Decline 6.3% in the Fourth Quarter, According to IDC, IDC (Feb. 1, 2018), https://www.idc.com/getdoc.jsp?containerId=prUS43548018.

[13] Ben Sin, *Huawei Doesn't Need America To Keep Growing*, FORBES (Jan. 12, 2018), https://www.forbes.com/sites/bensin/2018/01/12/the-american-governments-paranoia-about-huawei-wont-stop-the-chinese-tech-giants-growth/ (noting that Huawei distributes products to over 170 countries).

[14] Stu Woo, Ericsson, *Humbled by Huawei, Takes Another $1.8 Billion in Charges Swedish telecom-equipment maker adds to billions in charges amid turnaround effort*, WALL ST. J. (Jan. 16, 2018), https://www.wsj.com/articles/ericsson-humbled-by-huawei-takes-another-1-8-billion-in-charges-1516104065.

expensive equipment made by other firms.[15] Therefore, if the Commission decides to pursue these proposed rules, it is important to develop a clearer and focused policy that addresses real harms while limiting uncertainty and compliance burdens for USF recipients.

II. The Proposed Rules are Vague and Could Create Unintended Consequences.

The NPRM poses concerns, among other things, due to its lack of clarity regarding which companies would be barred. This reflects the difficulty in determining where threats could appear within a network, particularly when considering the various components and supply chain. As Dr. Charles Clancy, Professor of Electrical and Computer Engineering at Virginia Tech, testified recently before the House Energy and Commerce Committee's Subcommittee on Communications and Technology: "Supply chains for telecommunications are complex. They include development of intellectual property and standards; fabrication of components and chips; assembly and test of devices; development of software and firmware; acquisition, installation, and management of devices in operational networks; and the data and services that operate over those networks."[16] Furthermore, Dr. Clancy stated that "supply chain operations are among the most pernicious and difficult to detect."[17] The difficulty in locating points of vulnerability is a key reason why CCIA urges the Commission to be cautious and not rush into enacting vague rules,[18] which could lead to unintended consequences.

---

[15] Drew FitzGerald and Stu Woo, *In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser*, WALL ST. J. (Mar. 27, 2018), https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000.

[16] *Telecommunications, Global Competitiveness, and National Security: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. on Commc'ns & Tech.*, 115th Cong. (May 16, 2018) (testimony of Dr. Charles Clancy Professor of Electrical and Computer Engineering, Virginia Tech), https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-ClancyC-20180516-U11.pdf.

[17] *Id*.

[18] *See NPRM* at ¶ 13 ("We propose to adopt a rule that, going forward, no USF support may be used to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.").

A. The Commission Should Be More Precise Regarding the Application of its Proposed Rules.

It is unclear how the Commission would determine which companies would be barred from receiving USF benefits pursuant to the proposed rules. The NPRM has suggested: "One bright-line approach would be to prohibit use of USF funds on any purchases whatsoever from companies that have been identified as raising national security risks."[19] However, the Commission has left open how that determination would be made regarding "national security risks." One proposal is to bar:

> (1) any company that has been prohibited from bidding on a contract, participating in an auction, or receiving a grant by any agency of the Federal Government, for reasons of national security, or
> (2) any company from which any agency of the Federal Government has been prohibited by Congress from procuring or obtaining any equipment, system, or service that uses telecommunications equipment or services provided by that company as a substantial or essential component of any system, or as critical technology as part of any system.[20]

This language could be applied in a potentially overbroad manner. First, it could implicate companies that may have been barred for a reason not related to the supply chain issue. Second, it is unclear whether "any company" refers to a particular company that Congress has specifically barred from contracting with the Federal Government for national security reasons or to a company that has used equipment from another company that has been barred from contracting with the Federal Government for national security reasons.

Furthermore, the phrase "any system" is imprecise and raises concerns regarding the difficulty of determining where the vulnerabilities are in a network and which components or equipment would be implicated. For example, the proposed language could be read to bar a

[19] *Id*. at ¶ 15; *see also id*. at ¶ 19 ("We seek comment on how to identify companies that pose a national security threat to the integrity of communications networks or the communications supply chain for purposes of our proposed rule.").
[20] *Id*. at ¶ 20 (separation between points (1) and (2) added).

company if it has interconnected or used a network overseas not be subject to the same constraints as U.S. networks. That company could be implicated if the overseas network has some "telecommunications equipment or services" with "a substantial or essential component of any system, or as critical technology as part of any system" provided by a company that has been "prohibited by Congress".[21]

The NPRM next suggests applicability to companies that are "specifically barred by the National Defense Authorization Act from providing a substantial or essential component, or critical technology, of any system," or similarly "those that the National Defense Authorization Act specifically bars from developing or providing equipment or services, of any kind listed in the NDAA, to be used, obtained, or procured by any federal agency or component thereof."[22] However, the NPRM only refers to the FY 2018 NDAA, which could leave the Commission with a static list.

The NPRM also suggests that "a federal agency other than the Commission [would] maintain a list of communications equipment or service providers that raise national security concerns regarding the integrity of communications networks or the communications supply chain."[23] While this list may be more likely to remain timely, it is still very unclear which agency or agencies would decide how companies might be assessed for inclusion. Ultimately, CCIA believes that the Commission should coordinate its efforts across all Federal Government initiatives to create a more comprehensive policy, allowing other agencies with expertise to weigh in and help ensure that there are not competing or conflicting "blacklists."

[21] *Id*.
[22] *Id*. at ¶ 21.
[23] *Id*. at ¶ 22.

B. The Commission Should Be Cognizant of Risks in Banning Certain Equipment.

As an alternative to simply prohibiting USF funds from being used on purchases from companies deemed to raise national security risks, the NPRM proposes "to limit the scope of the proposed rule to equipment and services that relate to the management of a network, data about the management of a network, or any system the compromise or failure of which could disrupt the confidentiality, availability, or integrity of a network."[24] Although distinguishing based on equipment or services could be more precise in terms of addressing vulnerabilities in particular parts of a network, it may be difficult for USF recipients to know from which companies they are to purchase equipment, which could have an outsized impact on smaller, rural carriers. As mentioned before, to the extent that Huawei equipment is on U.S. networks, it is more likely to be found on the networks of smaller, rural carriers. Therefore, the Commission should be cognizant that a ban on certain networking equipment could actually widen the digital divide by cutting off a U.S. network provider's ability to purchase equipment or removing a source of necessary subsidies.

III. Conclusion.

CCIA appreciates that the "proposed rule or any alternative to restricting the use of USF funds that [the Commission would] adopt in this proceeding would apply only prospectively".[25] This would help alleviate a potentially massive compliance and technical burden for network providers. However, the proposed rules would create uncertainties that could hamper network providers. The Commission needs to be specific about not just the applicability of the rules themselves to certain companies and equipment, but also be clear in its scope. Vagaries in the

[24] *Id*. at ¶ 15.
[25] *Id*. at ¶ 17.

drafting of this policy could create uncertainties for USF recipients and U.S. companies in the supply chain. More importantly, there remains a lack of clarity about the scope of issues related to supply chain vulnerabilities – let alone the types of equipment and services or the companies that could be implicated by this rulemaking. Instead of rushing to a policy goal, the Commission should continue to study this issue, and, at the very least, issue a Further Notice of Proposed Rulemaking.

June 1, 2018

Respectfully submitted,

/s/ John A. Howes, Jr.
Policy Counsel
Ryan Johnston
Legal Fellow
Computer & Communications Industry Association (CCIA)
655 15th Street, NW Suite 410
Washington, D.C. 20005
(202) 783-0070
jhowes@ccianet.org